

## **II. General Remarks Concerning This Response**

Claims 1-3, 5-11, 13-19, and 21-24 are currently pending in the present application. Claims 1, 2, 5, 9, 10, 13, 17, 18, and 21 have been amended; no claims have been added; and claims 4, 12, and 20 have been canceled in this response. Reconsideration of the claims is respectfully requested.

## **II. Summary of Present Invention**

The present invention is a method, system, apparatus, or computer program product for providing secure session management using single-use tokens, also termed single-use cookies. After a single-use token has been issued to an entity, the entity may present the token to a service, and the receiving entity may identify the presenting entity based upon the presented token. However, the token may be used only once, after which the token must be updated or refreshed prior to re-use, thereby causing the token to be essentially reissued upon each use. The token comprises a session identifier of some sort that allows the issuer of the token to perform session management with respect to the receiving entity.

## **III. 35 U.S.C. § 102(e) - Anticipation**

The Office action has rejected claims 1-24 under 35 U.S.C. § 102(e) as anticipated by Reiche, U.S. Patent No. 6,092,196, "HTTP distributed remote user authentication system", filed 11/25/1997, issued 7/18/2000. This rejection is respectfully traversed.

Independent claim 1, as amended, reads:

1. A method for controlling access to protected resources within a distributed data processing system, the method comprising:

receiving at a first server from a client a request to access a protected resource and a single-use token associated with the client or a user of the client;

validating the single-use token, wherein the single-use token comprises session information for performing session management with respect to the client;

determining that the single-use token is a domain token;

generating a client authorization credential request; sending to a second server the client authorization credential request, the single-use domain token associated with the client or the user of the client, and a single-use domain token associated with the first server, wherein the first server and the second server are operated within a common domain;

generating a response to the request; refreshing the single-use token; and sending the response and the refreshed single-use token to the client.

As an initial point, Applicant notes that although Reiche discloses the usage of cookies, Reiche does not disclose the usage of single-use cookies, as required by the claim language of the present application, which recites an analogous data item, a token. The Office action states that Reiche discloses this feature in a portion at column 4, lines 55-60, which reads:

When a user is desirous to access a resource on a given customer server, say through HTTP data exchange session, the browser on the user's machine makes a first contact with the customer server. Access to the resource that is being sought is not permitted by the customer server since an access grant control transaction has not yet been completed, in other words, the customer server does not know if the request made by the user is legitimate.

This feature is supposedly also disclosed by Reiche in a portion at column 10, lines 15-67; Applicant notes that the relevant portion at column 10, lines 44-49, reads:

The row ID, client ID and transaction ID are determined from the cookie and, at step 262 and 264, are verified against the memory table 122. In addition, the number of transactions completed is checked (step 266) and the number of transactions left is decremented by one (step 268).

Thus, Reiche discloses that cookies are used for session management, and an aspect of session management in the system of Reiche is the limitation of the number of transactions that are performed for a client, but the cookies are not restricted to a single use. The usage of single-use tokens in the present invention is important because each time a client sends a request to the first server or the second server, the accompanying token is updated or refreshed, thereby modifying it; this single-use restriction is part of the overall domain security scheme.

More importantly, in the present invention, when a client is referred by a first server to a second server within the same domain for an authentication credentials request, the first server sends along its own single-use token to the second server. For example, the first server may send an authentication credentials request directly from the first server to the second server, or the first server may route the request by redirection through the client to the second server. In either case, the second server realizes that the request is coming from the first server, and the second server also requires that the first server sends along its single-use token. In this manner, requests from a client or from some other server in the same domain are treated equally; responses are not generated for requests unless they are accompanied by the appropriate single-use tokens, which are then refreshed by modification so that they are able to be used again. This feature is now clearly claimed in amended independent claim 1 by

incorporating the elements of original dependent claim 4 into claim 1. It should be noted that Applicant asserts that amended independent claim 1 is equivalent to original dependent claim 4 and does not introduce any new elements or limitations that were not previously presented by original dependent claim 4.

Reiche clearly does not disclose the features of claim 1, as amended, i.e. original dependent claim 4. In fact, the Office action omits any discussion of this feature; the Office action states on page 4:

sending to a second server the client authorization credential request, the single-use domain token associated with the client or the user of the client (see col 5, lines 1-53, Reiche discloses customer server exchange user ID information authentication server [sic] where HTTP associated with client); a single-use domain token associated with the first server, wherein the first server and the second server are operated within a common domain (see col. 10, lines 17-67, Reiche disclose cookie in HTTP customer server and authentication server network).

In the quoted portion of the Office action, the rejection notes that an HTTP cookie is sent by the client to the authentication server, i.e. the second server. The rejection then notes that the first server and the second server may be in a common domain. However, the rejection ignores the claim language in which the claim explicitly recites that a single-use token from the first server is also sent to the second server. In the system of Reiche, the transmitted cookie may have been set by the HTTP customer server, i.e. the first server, or by the authentication server, i.e. the second server. In contrast, for the present invention, the request to the second server is accompanied by the client's single-use token and also by the

first server's single-use token. There is no analogous or equivalent feature that is disclosed in Reiche that requires the authentication server in the system of Reiche to receive tokens for both the client and the customer server.

5        This feature, and the failure of the rejection to address it, becomes more prominent with respect to dependent claim 5. In dependent claim 5, both tokens from the client and the first server are validated by the second server, refreshed by the second server, and then returned by the second server. The  
10    Office action only refers to general language in Reiche about cookies without addressing the explicit claim language in claim 5 of the processing of two tokens, one from the client and one from the first server. Applicant asserts that the rejection fails to address the claimed elements because the rejection  
15    cannot refer to Reiche to find these features as Reiche does not disclose them.

Moreover, the importance of the multiple single-use domain tokens becomes more prominent in other dependent claims that contain claim elements that are directed to the distinction of  
20    single-use domain tokens and single-use service tokens. A server may receive and process multiple tokens and multiple types of tokens, as explicitly recited in dependent claim 2 or dependent claim 6. The Office action fails to address this distinction and merely continues to refer to the disclosure in  
25    Reiche of the use of typical cookies.

Reiche clearly does not disclose features as required by the language of the amended independent claims of the present application. As stated at MPEP § 2131: "A claim is anticipated only if each and every element as set forth in the claim is  
30    found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir.

1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Hence, for this and other reasons, Reiche cannot be used as an anticipatory reference, and the anticipatory rejections of the claims have been overcome, whereby Applicant requests the withdrawal of the rejections.

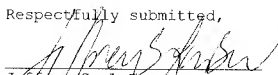
#### **IV. Conclusion**

It is respectfully urged that the present patent application is patentable, and Applicant kindly requests a Notice of Allowance.

For any other outstanding matters or issues, the examiner is urged to call or fax the below-listed telephone numbers to expedite the prosecution and examination of this application.

5      DATE:    September 26, 2006

Respectfully submitted,

  
Jeffrey S. LaBaw

Reg. No. 31,833

10      ATTORNEY FOR APPLICANT